ABSTRACT OF THE DISCLOSURE

The present invention provides an apparatus and method for performing cryptographic operations on a plurality of input data blocks within a processor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a cryptographic instruction and execution logic. The cryptographic instruction is received by a computing device as part of an instruction flow executing on the computing device. The cryptographic instruction prescribes one of the cryptographic operations, and also prescribes that an intermediate result be generated. The execution logic is operatively coupled to the cryptographic instruction. The execution logic executes the one of the cryptographic operations, and generates the intermediate result.